The HIPAA Implementation Newsletter
Issue #29 – March 8, 2002
Anniversary | What is HIPAA? | Status of Regs | Transactions | Privacy | Security
Web format with links at http://lpf.com/hipaa

This is the one-year anniversary issue of The HIPAA Implementation Newsletter. Issue #1 was sent out on March 9, 2001. Thank you for your continuing support and for passing the newsletter along to others who have subscribed. We are looking forward to another year of working with you in meeting the challenges of HIPAA.

___What is HIPAA?___

We have answered the question: What is HIPAA? so many times that we wrote
our answer down and posted it. If it works for you, please feel to use it. We will keep it current as regulations change, old issues are solved and new issues evolve.
http://lpf.com/hipaa/what-is-hipaa.html

___Status: Pending Regulations___

"HHS staff presented an update at the February, 2002 meeting of the NUCC/NUBC on the department's progress towards publishing the next round of
final and proposed HIPAA rules. Announced projections included:"
* Spring 2002: final Employer Identifier; proposed Modifications to Standards for Electronic Transactions (modifies pharmacy transaction standards) and proposed Revision to Transactions and Code Set Standards (adopts recent DSMO-recommended modifications)
* Spring/Summer 2002: final Security Standards and proposed Standard for Claims Attachments
* Summer 2002: final Provider Identifier and proposed Health Plan Identifier
+ More including link to compliance calendar
http://www.hipaadvisory.com/news/

___Transactions: Delays Q&A___

The Centers for Medicare and Medicaid Services has issued a document answering two-dozen frequently asked questions about the Administrative Simplification Compliance Act. The initial Q&As are introductory. The later Q&As are probably more useful to readers of this Newsletter.
+ More at: http://lpf.com/hipaa/ASCA-FAQs-1-31-02.html

___Transactions: Testing! Testing!___
TESTING! TESTING! DO YOU READ ME?

"The Centers for Medicare & Medicaid Services (CMS) white paper on testing seeks to clarify the ... the magnitude of this endeavor, and provide guidance in survival tactics ...

"... With HIPAA, the world changes. Even with a year's extension of the deadline for HIPAA (based on the submission of the required Compliance Plan)
most States will be burdened with the demands of increased testing. States rallied to the testing challenges of the Year 2000, but with HIPAA, internal and external testing requirements will greatly increase, not only in number, but in complexity as well.

" ... all the HIPAA transactions must be tested with multiple trading partners as well as in-house. Complex and rigorous testing is the key to insuring success whereby the standards mandated by HIPAA result in overall improvement of business processes.

"In order to adequately test HIPAA requirements, health plans will have to test with a large number of transaction submitters, and providers will have to test with many health plans. It is expected that this testing will be more demanding than any ever before experienced by the health care industry.
The use of a third party to certify compliance with HIPAA Implementation Guides can reduce the timeframe and cost involved in testing by substantial elimination of point-to-point testing. This cost reduction is highest when significant numbers of data trading partners, e.g., providers and clearinghouses, have also used a certification service. This results in reduction of the cost of implementation for both providers and payers.

"Even if ... software has been 'factory certified' as complying in every detail with the requirements of the Implementation Guides, it must still be tested again once it is installed in the organization's system. First of all, 'factory certification' only assures that the product contains the format and code set rules of the guides. Once installed, it must be tested to verify that the mapping of the client's data to the X12N fields is accurate and that additional functions provided by the translator are correctly performed. The additional functions include conversion of standard to local codes where possible and when necessary, and stripping and storing of data not needed for transaction processing, but required to construct an outbound transaction.

"What makes the whole Business-to-Business testing even more complicated is
the issue of sequencing. If all entities were ready to test all transactions at the same time, there would still be a massive problem of planning the tests. But if all entities are focusing on different transactions at any point in time, there will be chaos! In response to the original deadline,

WEDI SNIP proposed a national plan to sequence the transactions so that across the country, each entity would be testing the same transaction at the same time. [Available at: http://snip.wedi.org/public/articles/Trans0615.pdf]

"The primary message of the paper is that HIPAA implementation testing far exceeds any previous testing experience including Y2K in terms of breadth, volume, complexity, and numbers of required tests. "
+ More at: http://www.hcfa.gov/medicaid/hipaa/adminsim/vol2map3.pdf

___Transactions: Myths & Realities___
HIPAA'S Myths, Practical Realities And Opportunities: The Work Providers Need To Perform For Standard Transactions And Code Sets – PricewaterhouseCoopers January 2002

Eight myths are explored in depth (39 pages):
1. The only thing physicians, hospitals and other health care providers need to do is to contract with a clearinghouse to achieve HIPAA compliance.
2. Vendors can deliver HIPAA compliance to providers via software.
3. Many providers are already HIPAA compliant with these transactions, what'
s the big deal
4. The industry will have had more than the required 24 months to implement
administrative simplification.
5. Medicare already does it, therefore it should translate easily into other government and private pay situations.
6. HIPAA compliance will be much simpler for small providers.
7. State governments only need to worry about Medicaid and their state employee group health plans.
8.HIPAA compliance equals administrative simplification.

As an example of the depth of the analysis, here is a brief portion of the analysis of myth #3 that supports some of the other material in this issue:
"... most providers have overlooked the critical need for testing. Providers need to conduct testing with each payer for a variety of transactions, not only for the format and content that is specifically required, but also for any optional data elements that may be agreed to contractually. In addition, many provider systems currently contain logic to create payer-specific coding to accommodate payer or plan-specific code sets. With the elimination of non-standard codes, providers must 'unwind' payer-specific coding issues and implement new process to track and submit non-standard yet required data. We are particularly concerned that few providers have assessed the effect this code set conversion will have on their specific reimbursement levels."
+ More at:
http://www.pwchealth.com/cgi-local/hcregister.cgi?link=pdf/hipaa_myths.pdf

___Privacy: California___

"... the California HealthCare Foundation released a series of guides designed to help California health plans, providers, and pharmacists understand the requirements of the new Federal Health Privacy Rule. The guides, written by the Health Privacy Project, explain how the Privacy Rule issued under HIPAA interact with existing California privacy law. ... The guides are available for download from the Foundation's Web site
+ More at: http://www.chcf.org

"The guide is meant to serve as a general road map for implementing the Privacy Rule and will help providers begin the process of determining what steps they will need to take to come into compliance with the Privacy Rule in April 2003." The guide for health care providers is 46 pages long. The guide for insurers is 58 pages. They should be useful even if you are not a California provider or plan.

The guides note the requirement to "develop policies and *practices* reasonably assuring that the minimum amount of health information necessary
is used or shared." (p 13 both guides, emphasis added). Appendix B in both guides provides a Checklist for Key Items that references both policies and training, but not practices. In your planning, do not overlook the calendar time it will take to get policies developed, reviewed and approved, to then determine what changes in practices are needed to implement the policies, to develop new practices including both system changes and manual procedures,
to test them, train people and get the new practices imbedded in day-to-day operations. And, privacy without supporting security will not meet the HIPAA requirements. Security to support privacy must meet at least the "good business judgement" standard. The required coordination and changes in human
behavior can be very time consuming.
+ More at:
http://admin.chcf.org/documents/ehealth/ImplementingFedPrivacyRuleProviders.
pdf
http://admin.chcf.org/documents/ehealth/ImplementingFedPrivacyRulePlans.pdf

___Security: Hospitals Boosting Data Security___

"Pending HIPAA requirements to ensure the security of health care information along with increasing security threats are driving boosts in hospital spending for data security technology, according to a survey from Porter Research, an Alpharetta, Ga.-based consulting firm.
"In the survey of CIOs from 100 hospitals, 93% of respondents listed HIPAA as one of the primary reasons for higher security budgets. Another 52%

listed increased security threats, and 10% cited accreditation requirements. Some 21% of respondents acknowledged having a firewall breached while only
7% said their hospital was "very prepared" to ward off security breaches.
"Security technologies currently in use at hospitals, according to survey respondents, include anti-virus software (100%), firewalls (96%), virtual private networks (83%), data encryption (65%), intrusion detection (60%), vulnerability assessment (57%), public key infrastructure (20%) and biometrics (10%). Virtually all respondents expected to use all of these technologies to some degree during the next two years.
"To protect clinical data, 73% of respondents report using some type of security technology for medical records, followed by radiology (64%), pharmacy (64%), patient care (61%), scheduling (54%), computer-based patient
records (50%), decision support (42%), hand-held technologies (33%), case management (27%) and disease management (16%).
"Asked to rate their awareness of 21 data security vendors, respondents showed little brand awareness of this sector, according to the survey. Some 42% of respondents said they "know well" the vendor VeriSign, followed by Pyxis (35%), RSA (28%), Network Associates (27%), Trend Micro (16%), Watch
Guard (13%), Internet Security System (9%) and Entrust (9%). While vendor
brand awareness may be low, CIOs rank technical knowledge and reputations as
top criteria for selecting a vendor partner." (February 26, 2002)
+ More at:
http://www.healthdatamanagement.com/html/news/NewsStory.cfm?DID=7912

___Security: Intrusion Detection Perspective___
"Intrusion detection allows organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security professionals should not be whether to use intrusion detection, but which intrusion detection features and capabilities to use. IDSs have gained acceptance as a necessary addition to every organization's security infrastructure.
"By increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system, an IDS can serve as a significant deterrent to insiders who would violate an organization's information security policy.
"Despite the positive impact it can have on an organization, no IDS is indestructible and certainly should not be the only security measure that an organization employs. Only by combining an IDS with other countermeasures—such as firewalls, VPNs, and antivirus products—does an organization protect from a realistic range of security attacks. This combination is sometimes called security in depth or defense in depth."

+ More at: http://www.gartner.com/DisplayTechOverview?id=320015 and http://www.gartner.com/resources/95300/95367/95367.pdf

___Security: Intrusion Detection 101___

"… There are two basic types of intrusion detection: network-based and host-based. Network-based systems examine each packet of information, looking for protocol anomalies and known virus signatures. Host-based systems, which are used for individual machines as opposed to networks, read
log files, look for inadvisable settings or passwords, and other potential policy violations.

"Intrusion detection picks up where firewalls leave off. It can be especially critical for enterprises that rely heavily on the Internet to conduct business, said John Pescatore, research director for Gartner Group in Stamford, Conn. "Firewalls do a good job of keeping the 'bad guys' out. Once you start using inbound connections, like e-business or remote access, you poke holes in that firewall. Intrusion detection is a way to make sure that only the 'good guys' remotely access your network.

"Generally our advice is to start with network-based IDS at the trust boundaries, like your connections to … business partners," said Pescatore. "The biggest reason (to start small) is that it takes a lot of work to monitor intrusion detection, especially when you first get started.

"Indeed, adding intrusion detection can be like "getting a Christmas puppy," said Pete Lindstrom, director of security strategies for Hurwitz Group of Framingham, Mass. "It sounds like a wonderful idea, until you go and visit your in-laws and you come back to find it's peed in the corner and torn up your couch."
+ More at:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci80227
8,00.html

___Security: The Legal Risks of Computer Pests___

"Computer Pests are malicious programs that go beyond typical viruses. Pests
are a legal threat to corporations with sites on the Internet. This paper describes the threats in terms of vicarious liability, negligence, regulation, negative publicity and liability to shareholders. Corporations have abundant incentive to treat Pests with vigilance. Although many don't think about it, it is common sense that managers should have a legal responsibility to police what is happening within their computer systems. This responsibility is manifest through different particular laws in different situations. As computer systems assume an ever-larger role in

modern society, the legal system is responding by holding the custodians of those systems accountable for security. The person enforcing that accountability might be a regulator, a shareholder, an employee, a customer or anyone – including a fellow corporate resident of the Internet -- who suffers on account of lax security."
+ More at: http://www.pestpatrol.com/Whitepapers/LiabilityofPests.asp and http://www.pestpatrol.com/Whitepapers/Index.asp

___HIPAA Conferences___

HIPAA Summit West II March 13 - 15, 2002 San Francisco, CA
http://www.hipaasummit.com/HIPAAWest2/index.php3

The Fourth Nationa lHIPAA Summit April 24-26, 2002 Washington, D.C.
http://www.hipaasummit.com/HIPAA4/index.php3
The HIPAA Summit conference series provides a road map to understanding the
complex requirements of federal and state law and illuminates strategies for compliance. Through an expert faculty of over 100 and over 45 concurrent sessions, the Fourth National HIPAA Summit will provide the most up-to-date
and sophisticated information on the status and construction of the HIPAA regulations through the presentations of the leading HIPAA regulators from the Department of Health and Human Services. Further, the Summit will provide specific and in-depth analysis of the healthcare privacy and security laws of a number of major states. The Fourth National HIPAA Summit
will focus on practical case studies from the field, featuring presentations by leading privacy, security and compliance officers from around the country. Finally, the Summit will address the complex financial, operational and technical issues that must be addressed not only to comply with the technical requirements of the law, but also to integrate new technologies in order to enhance the efficiency, quality and accessibility of healthcare services.

_____

To be removed from this mail list, click:
mailto:hipaa@lpf.com?subject=remove
To subscribe, click: mailto:hipaa@lpf.com?subject=subscribe We appreciate it
if you include information about your firm and your interests.

Information in the HIPAA Implementation newsletter is based on our experience as management consultants and sources we consider reliable. There
are no further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals.

Lyon, Popanz & Forester http://lpf.com is a management consulting firm that designs and manages projects that solve management problems. Planning, program management offices and project management for HIPAA are areas of
special interest.